AO 106 (REV 4/10) Affidavit for Search Warrant

AUSA Sean Franzblau, (312) 353-5305

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

The cellular telephone, further described in Attachment A2

Case Number:

21M547

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Gregory B. Linder, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A2

located in the Northern District of Illinois, there is now concealed:

See Attachment B2

The basis for the search under Fed. R. Crim. P. 41(c) is evidence.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Sections 666(a)(1)(B) and 666(a)(2)	federal program bribery

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.

Gregory B. Linder by [illegible]
Applicant's Signature

GREGORY B. LINDER, Special Agent
Federal Bureau of Investigation
Printed name and title

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: August 13, 2021

[illegible]
Judge's signature

City and State: Chicago, Illinois

GABRIEL A. FUENTES, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Gregory B. Linder, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation. I have been so employed since approximately 2016. I am currently assigned to a public corruption squad, the primary purpose of which is to identify and investigate public corruption and bribery-related conduct by public officials. Through my training and experience, I am familiar with the techniques used to investigate such violations, including consensual monitoring, surveillance, data analysis, and interviewing witnesses and others who have knowledge of the corrupt activities. I have also participated in the execution of numerous federal search warrants.

2. This affidavit is made in support of an application for (1) a warrant to search a gray Apple iPhone XS cellular telephone, assigned International Mobile Equipment Identity (IMEI) number 357202093093541 and telephone number [redacted] [redacted] ("**Subject Phone**") for evidence described further in Attachment B, concerning federal program bribery offenses, in violation of Title 18, United States Code, Sections 666(a)(1)(B) and 666(a)(2) (the "**Subject Offenses**"); and (2) a warrant to search the person of [redacted] for purposes of seizing the **Subject Phone**, which was used as an instrumentality of the **Subject Offenses**.

3. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from

persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing two search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence of violations of Title 18, United States Code, Section 666(a)(1)(B) and 666(a)(2), are located within the **Subject Phone**, and that the **Subject Phone** is likely to be in the possession of [redacted]

I. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH THE SUBJECT PHONE

A. Factual Background

4. On or about July 24, 2020, the government applied for a warrant to search (the "[redacted] application") the iCloud account for Apple ID [redacted]sbcglobal.net (the "[redacted] iCloud Account"). The [redacted] application is attached to this application as Exhibit 1 and is incorporated herein by reference. The [redacted] application established probable cause that: (1) the [redacted] iCloud Account was used by [redacted] a private Chicago businessman; (2) in or around 2019, [redacted] made at least two concealed payments to [redacted] in exchange for [redacted] interfering with a development project in the [redacted] that was against [redacted] interests ("the Project"), in violation of the **Subject Offenses**; and (3) evidence of [redacted] and [redacted] violations of the **Subject Offenses** was then contained within the [redacted] iCloud Account.

5. In summary, as explained in further detail in the [redacted] application, the FBI has developed a confidential source (CS-1) who was [redacted]

Avenue in Chicago, including approximately $16,000 worth of window replacements. According to CS-1, s/he explained to [redacted] that he could not use City funds to pay for the renovations, and [redacted] responded that [redacted] was going to pay for the window renovations. Ex. 1, ¶ 23. On the morning of May 11 or May 18, 2019 (CS-1 was certain it was a Saturday morning but could not recall which date), CS-1 observed [redacted] hand [redacted] an envelope containing $5,000 in cash that [redacted] used to pay the owners of his [redacted] office building for the window replacements later the same day. *Id.* at ¶¶ 24-27.[1] According to CS-1, [redacted] took steps to conceal the payment, including by asking the owners of his [redacted] office building to not record the payment, and not reporting the payment in his [redacted] reports because [redacted] had instructed him not to. *Id.* at ¶¶ 27-28. On at least one other occasion within the following weeks, CS-1 saw [redacted] meet with [redacted] privately outside of his office, and return carrying a stuffed envelope that appeared similar to the envelope containing $5,000 that [redacted] had previously received from [redacted] *Id.* at ¶ 29.

---

[1] CS-1's information is corroborated in part by a May 11, 2019 text message conversation recovered from CS-1's phone between [redacted] and CS-1 in which they appear to discuss an upcoming meeting with the building owners at which the window replacements were to be discussed:

> [redacted] (9:27 a.m.): What time we meeting today w [redacted] [CS-1 has explained [redacted] is a nickname used by one of the owners of the building in which [redacted] office is located].
>
> CS-1 (9:27 a.m.): 10 am I got it.
>
> [redacted] (9:29 a.m.): I will have the guy who is installing the windows in the meeting w us.

7. According to CS-1, in or around May and June 2019, shortly after [redacted] received the $5,000 from [redacted] the window replacements were completed at [redacted] office. As explained at paragraph 30 of the [redacted] application, CS-1 provided agents with several photographs that CS-1 stated s/he received from [redacted] which appeared to depict the window replacement/associated renovation work at the [redacted] office at various phases. Further, City of Chicago records show that a building permit to replace windows at [redacted] office was issued on May 13, 2019. Ex. 1, ¶ 31.

8. According to CS-1, months later, in [redacted] instructed CS-1 to draft a statement to announce formally [redacted] opposition to the Project, which, based on the [redacted] effectively stopped the Project [redacted] Ex. 1, ¶¶ 49-50. According to CS-1, [redacted] told CS-1 to say in the statement that he was opposing the Project based on feedback he had received from the public. *Id.* at 49. According to CS-1, that did not make any sense because the Project appeared to have the strong support of the vast majority of [redacted]. *Id.* According to CS-1, minutes after [redacted] told CS-1 to draft the statement, [redacted] stated words to the effect of, "[Project developer] likes tying up [redacted] money, let's see how he likes it done to him." *Id.* at ¶ 50. As explained in detail throughout the [redacted] application, substantial independent evidence, including bank records, toll records, and a text message from [redacted] to CS-1 concerning [redacted] and the Project, generally

corroborate CS-1. *See, e.g., Id.* at ¶¶ 32-40, 51.

9. On or about July 24, 2020, the Court issued the [redacted] warrant, which, among other things, authorized the government to search all Short Message Service (SMS) and Multimedia Message Service (MMS) text messages sent to or from the **Subject Phone** between February 2019 and July 24, 2019 for evidence of the **Subject Offenses.**[2] [As explained in detail in the [redacted] application, [redacted] is the user of the **Subject Phone**, and the **Subject Phone's** data was backed up to the [redacted] iCloud Account during the relevant time period, *see* Ex. 1, ¶¶ 32-33, 65].

B. Execution of the [redacted] Warrant and the Unrecoverable MMS Messages

10. On or about July 24, 2020, the FBI served the [redacted] Warrant on Apple. On or about August 3, 2020, Apple produced the returns in an encrypted format. The encrypted files were then provided to a unit within FBI headquarters to be decrypted. The decrypted files were returned to FBI-Chicago on or about August 24, 2020. At that point, the decrypted files were provided to the FBI's Regional Computer Forensics Laboratory (RCFL) to be analyzed and formatted so that the case agents, including myself, could review the files on a software program used to review the download of digital devices and iCloud content. This review and formatting was

---

[2] Based on my training and experience, I know that SMS messages are electronic messages that generally contain text only. MMS messages contain multimedia content, including pictures, videos, audio recordings (including voicemails), and contact information. If multimedia content is sent in tandem with text content, the message is typically sent as one MMS.

completed on or about October 13, 2020.

11. The RCFL forensic analysis revealed that [redacted] sent or received thousands of Short Message Service (SMS) text messages and Multimedia Message Service (MMS) during the period covered by the [redacted] warrant (February 2019 to July 2020). Due to an unexplained technological problem however, few of the MMS messages could be opened or reviewed (the "unrecovered MMS messages").[3] Nevertheless, the forensic analysis did reveal the existence of the unrecovered MMS messages, including the date and time the messages were sent/received, and the other numbers that the MMS messages were sent to/from. Based on this data, the case agents determined that [redacted] sent and received over approximately 4,000 MMS messages between February 2019 and July 2020, the vast majority of which agents were not able to view. Approximately 59 of the unrecovered MMS messages were sent between [redacted] and [redacted] Under the [redacted] warrant, agents were authorized to view all of the unrecovered MMS messages to determine if any were subject to seizure under the parameters of Section A.III. of the [redacted] warrant ("Information to be Seized by Law Enforcement Personnel").

12. Between November 2020 and June 2021, case agents, including myself, consulted with RCFL technicians and FBI computer scientists to determine why the unrecovered MMS messages were unviewable. Additionally, the assigned Assistant

[3] As explained below, agents were able to review the content of SMS messages sent to and from the **Subject Phone**, which led to the discovery of several communications related to the **Subject Offenses** between [redacted] and others.

United States Attorney consulted with an attorney and computer scientist at the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS). Based on these consultations, it was determined that the unrecovered MMS messages could potentially be recovered by the RCFL if it were provided with the original encrypted [redacted] iCloud Account returns produced by Apple on or about August 3, 2020 (as opposed to the decrypted version of those returns that were initially provided to the RCFL in or around August or September of 2020). On or about June 14, 2021, the original encrypted returns were provided to the RCFL. On or about June 16, 2021, the case agents were notified by an RCFL technician that he was unable to recover any of the unrecovered MMS messages from the original encrypted returns. The RCFL technician then submitted the original encrypted returns to FBI headquarters in a final attempt to decrypt the original returns and recover the unrecovered MMS messages.[4] FBI headquarters returned the decrypted files to FBI-Chicago on or about June 30, 2021. I reviewed these files on or about July 7, 2021 and determined that nearly all of the unrecovered MMS messages were still unviewable.

13. Because reasonably diligent efforts have failed to recover the unrecovered MMS messages from the original [redacted] iCloud Account returns, the government now seeks warrants authorizing it to seize the **Subject Phone** from [redacted] and search the **Subject Phone** for the unrecovered MMS messages.

[4] This was done because, according to RCFL personnel, there was a possibility that updates in decryption technology at FBI Headquarters would allow for the recovery of the missing MMS messages.

C. The Evidence Found Within the SMS Messages Recovered from the [redacted] iCloud Account Strengthen the Probable Cause that the Unrecovered MMS Messages Contain Evidence of the **Subject Offenses**

14. As explained above, the information contained in the [redacted] Application provided probable cause to search all of the unrecovered MMS messages for evidence of the **Subject Offenses**. That probable cause, however, has been significantly strengthened based on the content of the SMS messages recovered from the [redacted] iCloud Account, which corroborate CS-1 in several significant ways.

i. [redacted] and [redacted] Discussed the Project Several Times in the Weeks Leading up to [redacted] Formal Announcement of his Opposition

15. For example, a series of SMS messages sent between [redacted] and [redacted] in the week or so leading up to [redacted] announcement of his opposition to the Project on September 27, 2019 corroborate that [redacted] and [redacted] were discussing the Project shortly before [redacted] announced his opposition on September 27, 2019, and provide a reasonable basis to believe that [redacted] exercised improper influence over that decision:

September 17, 2019

[redacted] (9:22 p.m.): [redacted] great job representing the community tonight. I just left not sure how much longer it going to go but seem like there was a lot more people lined up to speak. [This is a reference to the September 17, 2019 community meeting at which Developers 1 and 2 and others presented the Project plan to community members, and [redacted] received public comment, *see* Ex. 1, ¶¶ 41-47].

[redacted] (10:25 p.m.): Thank you for coming!

September 22, 2019

[redacted] (10:21 p.m.): Let's schedule a meeting together before this Friday [September 27, the day [redacted] announced his opposition to the Project]. I'm meeting with [Developer 1's last name] Friday afternoon.

September 23, 2019

[redacted] (7:21 a.m.): I'm open today for lunch or anytime between 11 and two.

[redacted] (7:21 a.m.): Tomorrow I'm pretty much open all day.

[redacted] (8:44 a.m.): U wanna meet at 1230 in yr office?

[redacted] (8:47 a.m.): Sure I'll see you at [redacted] s, [redacted] business] today at 12:30 p.m.

[redacted] (12:02 p.m.): I may be a little late.

[redacted] (12:27 p.m.): I'm here.

[redacted] (12:27 p.m.): No problem.

[redacted] (12:28 p.m.): Be there in 5 mins. U want a coffee?

[redacted] (12:29 p.m.): Or something else?

[redacted] (12:29 p.m.): No I'm good thank you.

[redacted] (12:29): Whatever you're getting I'll get the same.

16. The above exchange is significant for several reasons. As explained in detail in the [redacted] warrant, [redacted] had no legitimate role in the Project, so it is unusual that [redacted] thought it necessary to meet with [redacted] an ostensibly disinterested party—to discuss the project in the days leading up to the formal announcement of [redacted] opposition (and prior to [redacted] presumably

final meeting with Developer 1 before the announcement). Second, based on my training and experience, it is unusual for a public official like [redacted] to meet with a [redacted] at the [redacted] (as opposed to the [redacted] office or some other public location) to discuss a matter of public concern. [redacted] apparent desire to meet alone at [redacted] office provides a reasonable basis to believe that he wanted to conceal their meeting.

ii. [redacted] and [redacted] met Frequently in the Spring of 2019, when CS-1 States s/he Saw [redacted] deliver cash payments to [redacted]

17. The SMS messages recovered from [redacted] iCloud Account also corroborate that [redacted] and [redacted] were frequently meeting with one another in the spring of 2019—when CS-1 says [redacted] received at least two large cash payments from [redacted] under similar circumstances to what CS-1 described. For example, as explained in the [redacted] Application (¶ 21-22) and in the background section above, CS-1 stated that on or about May 7, 2019, [redacted] introduced CS-1 to [redacted] at the [redacted] where [redacted] was working at the time. According to CS-1, during the meeting, [redacted] explained that [redacted] ([redacted] predecessor) had "screwed" [redacted] by convincing a local developer to build [redacted] facilities as part of the Project, rather than on a local property owned by [redacted] and that [redacted] had lost over $20,000 as a result. According to CS-1, during the meeting, [redacted] stated he was angry with [redacted] and the developers behind the Project and wanted to get back at them. CS-1 further stated

that, immediately after the meeting, [redacted] stated words to the effect of, "[redacted] has a lot of money, and he's going to be a good friend once I'm in office."

18. Agents recovered several text messages from the [redacted] iCloud Account that corroborate that [redacted] and [redacted] met at a Chicago fire station on May 7, 2019. Further, shortly after the meeting, [redacted] sent [redacted] one of the MMS messages that agents were unable to recover from the [redacted] iCloud Account returns:

May 7, 2019

[redacted] (5:06 p.m.): [redacted] I'm heading your way what's the address it at the [redacted] or what's the cross streets.

[redacted] (5:11 p.m.): [redacted]

[redacted] (5:12 p.m.): Ok.

[redacted] (8:36 p.m.): [[redacted] sends [redacted] an unrecovered MMS message].

19. As explained in further detail in the [redacted] Application (¶¶ 24-29), CS-1 stated that shortly after the May 7, 2020, fire station meeting, [redacted] met with [redacted] outside [redacted] [redacted] office on at least two occasions to receive envelopes full of cash (the first of which payment [redacted] used to pay the owners of his [redacted] office building to replace the windows). SMS messages recovered from the [redacted] iCloud Account reveal that [redacted] and [redacted] met with each other several times in May 2019, often in parking lots near [redacted] office. Further, [redacted] and [redacted] frequently exchanged MMS messages after these meetings, which messages were unrecoverable from the [redacted] iCloud Account

returns and which, based on my training and experience, likely contain information regarding what occurred at these meetings. For example, the following exchange took place on May 9, 2019 (two days after the [redacted] meeting):

[redacted] (8:20 a.m.): Good morning [redacted] do you have time to meet this morning?

[redacted] (9:24 a.m.): I am at the office. Be back soon.

[redacted] (9:48 a.m.): I am back.

[redacted] (9:49 a.m.): Walking to the lot.

[redacted] (9:51 a.m.): I'm in front of you.

[redacted] (9:53 a.m.): Where?

[redacted] (10:33 a.m.): [[redacted] sends [redacted] six unrecovered MMS messages].

20. On May 18, 2019, [redacted] and [redacted] exchanged the following SMS messages:

[redacted] (12:18 p.m.): I am with my wife doing errands and I am stopping by my moms around 130 then heading in your direction.

[redacted] (12:23 p.m.): Ok I am at [redacted].

[redacted] (3:06 p.m.): [[redacted] sends [redacted] an unrecovered MMS message].

iii. [redacted] was Heavily Involved in Planning the Renovations at [redacted] Office.

21. Next, the SMS messages corroborate that [redacted] was heavily involved in planning and overseeing renovations at [redacted] office in the

spring of 2019, which included the replacement of windows. *See* Ex. 1, ¶¶ 23-31). This is significant because, as explained in detail in the [redacted] Application, CS-1 stated that [redacted] told CS-1 that [redacted] was going to pay for the renovations. Ex. 1, ¶ 23. Further, there is substantial evidence that [redacted] took steps to conceal these payments, including by instructing his landlords and CS-1 not to record a $5,000 cash payment for window replacements that [redacted] received from [redacted] Ex. 1, ¶¶ 24-28.[5]

22. Specific SMS messages recovered from the [redacted] iCloud Account returns that corroborate [redacted] involvement in the [redacted] office renovations include the following:

- A May 8, 2019 text message from a third party to [redacted] (9:08 a.m.): "This is Tom with [redacted] can you please give me a call about [redacted] office[?] Can we meet there today anytime[?]"[6]

---

[5] On or about November 10, 2020, the Court issued a second search warrant (20 M 597) that allowed the government to seize a broader range of items from the [redacted] Warrant returns than what was originally covered in the [redacted] warrant. Specifically, whereas the [redacted] warrant authorized the government to seize "Communications with [redacted] related to . . . payments from [redacted] to [redacted] it did not specifically list communications related to the renovations/improvements at [redacted] office, nor did it include communications between [redacted] and third-parties regarding those renovations/improvements. While there was a reasonable basis to believe that [redacted] paid for the renovations (and thus communications about the renovations constitute evidence of payments from [redacted] to [redacted] out of an abundance of caution, the government sought to expand the scope of items to be seized so it more clearly covered all communications related to renovations at [redacted] office, including conversations between [redacted] and third parties.

[6] Based on a search of the Illinois Secretary of State website, [redacted], Inc. is a Chicago-based company owned by [redacted]. A general internet search for [redacted] glass and aluminum features for commercial and residential buildings.

- A May 9, 2019 text message from [redacted] to [redacted] (12:44 p.m.): "Call the concrete guy, he's waiting for your call."
- A May 10, 2019 text message exchange between [redacted] and "Tom" from [redacted]:
  - [redacted] (8:19 a.m.): "What do you think should he have it scraped and painted or should we just cover it would break metal[?]
  - [redacted] (8:20 a.m.): "Break metal would be faster and quicker or panel 15 just leave a few weeps holes."
  - Tom (8:20 a.m.): "We can do Breakmetals but lentil is totally gone it's gonna drop."
  - Tom (8:20 a.m.): "On big one only but we can install the window no problem."
  - Tom (8:21 a.m.): "Small window lentils are OK they just kept the water inside whoever did this at no idea how that works."
  - Tom (8:22 a.m.): "I think big lentil should be replaced somebody would have to look at that."
  - [redacted] (8:23 a.m.): "Can you call [redacted] and tell him to have the building owner look at that because the owner of the building should replace that[?]"
  - Tom (8:24 a.m.): "K"
  - Tom (8:39 a.m.): "[redacted] is going to talk to the owner and he's going with clear anodized so if you want to give him those couple doors we can probably use them if you want me to stop by I'll stop by to take a look. Let me know."
- A May 10, 2019 text message from [redacted] to [redacted] (8:24 a.m.): "[redacted] I told Tom from the glass company to call you[.] [T]he steel above the window's is rusted but some of the steel that's holding the brick needs to be replaced[.] [I]t's a dangerous situation[,] the building owner should take care of that."
- A May 18, 2019 text message from [redacted] to a third party (9:44 a.m.):

[M]y new [redacted] [is] asking if we have that emblem[,] I'm doing some concrete work for him right now and he wants to put it in the concrete."

- A May 18, 2019 text message exchange between [redacted] and [redacted]
  - [redacted] (12:17 p.m.): "How's the widows [sic] coming did he give you a good bricklayer[?]"
  - [redacted] (12:17 p.m.): "He is good."
- A July 2, 2019 text message from [redacted] to [redacted] "Ok, looking for a carpenter to do trim work around the windows."
- A July 3, 2019 text message response from [redacted] to [redacted] "Good morning [redacted] the carpenter cancelled on me this morning[,] we're rescheduling for next week."

23. There is independent evidence that [redacted] did not pay for the window replacements at his [redacted] office.[7] Specifically, I have completed a financial investigation of [redacted] that included a review of [redacted] D-2 [redacted] reports, [redacted] expense account, and all [redacted] known personal bank and credit card accounts. There is no record of [redacted] paying for renovations to his [redacted] office with any personal accounts, or with his [redacted] expense account. There is evidence of [redacted] paying for certain small-scale renovations/improvements for his [redacted] office

[7] At the time the government submitted the [redacted] application in July 2020, it had completed a financial review of [redacted] reports and [redacted] expense account (*see* Ex. 2, ¶ 31) but had not yet completed its review of [redacted] personal finances (personal bank account and credit cards). The government has since completed its review of [redacted] personal finances and confirmed there is no apparent record of payments for renovations/improvements to the [redacted] office (including window replacements) within [redacted] personal financial records.

with [redacted] but this does not appear to include the window replacements.

24. Specifically, [redacted] listed on his D-2 [redacted] reports three separate expenditures with the listed purpose as "Office buildout" for purchases at Lowe's Home Improvement, Home Depot, and [redacted] The total amount for the three expenditures was $3,726.94. There are no reported payments to [redacted] or any other apparent window or glass companies. Thus, financial records corroborate that a third party (someone other than [redacted] paid for the window replacements at [redacted] office.

25. I have completed only a partial financial investigation of [redacted] Specifically, I have obtained bank records for all of [redacted] known personal and business accounts. [redacted] accounts do not reflect any activity that is consistent with him paying for the window replacements at [redacted] office, or making a $5,000 cash withdrawal in or around May 11 or May 18, 2019. *See* Exhibit 2, ¶¶ 24, 33, 34. If [redacted] paid for the window replacements at [redacted] office, I believe it is most likely that he used money from a business account as it would be easier to conceal (as explained in the [redacted] Application, [redacted] himself owns a glass glazing company called [redacted]; there are obviously many ostensibly innocent reasons why a glass service-provider might be paying [redacted] a glass supplier). Further, because this investigation is still in a covert phase, I have not subpoenaed [redacted] directly for records concerning who paid for the renovations at [redacted] office.

iv. By May 18, 2019, [redacted] had done things for [redacted] that Made [redacted] feel Indebted to [redacted]

26. The SMS messages recovered from the [redacted] iCloud Account also demonstrated that by May 18, 2019, [redacted] had done certain things for [redacted] that made [redacted] feel indebted to [redacted] and [redacted] was starting to take certain non-official actions to reciprocate. This is highly significant because, as explained in detail in the [redacted] application, there is substantial evidence that the $5,000 payment that CS-1 observed [redacted] make to [redacted] occurred on the morning of May 11 or 18, 2020. *See* Exhibit 2, ¶¶ 24, 33, 34, These messages included a May 18, 2020 message sent from [redacted] to [redacted] (10:19 a.m.): "I want to take [yo]u and Conrad out to dinner. Wherever y[ou]r favorite place is."

27. The following day, May 19, 2020, [redacted] and [redacted] had a text exchange in which [redacted] provided [redacted] with a "floor ticket" to what is believed to be the inauguration ceremony of the newly-elected Chicago City Council members because [redacted] had been "very very good" to [redacted]

- [redacted] (8:13 p.m.): '[redacted] I got u a floor ticket U have been very very good to me. If u want to go, go. If not, but let me know.
- [redacted] (8:16 p.m.): "Ok I'm in[,] see you tomorrow."
- [redacted] (8:26 p.m.): "U still want me to put it in yr mailbox right?"

---

[8] May 19, 2019 is one day after agents believe, based on information provided by CS-1 and corroborating bank records, [redacted] made the $5,000 cash payment to [redacted] that CS-1 observed.

- [redacted] (6:27 p.m.): "Yes."
- [redacted] (10:16 p.m.): I put ticket inside yr door."
- [redacted] (10:16 p.m.): "Floor ticket."
- [redacted] (8:39 a.m. on May 20, 2019): "Thank you."

D. There is Probable Cause to Believe that the Subject Phone Currently Contains at least some of the Missing MMS Messages

28. Based on my review of subscriber records received from Verizon, I know that [redacted] used the **Subject Phone** during the entire period covered by the [redacted] warrant (February 2019 to July 24, 2020), and that [redacted] has continued to use the same device as of August 4, 2021. Specifically, based on my training and experience, I know that all cellphones are assigned a unique International Equipment Mobile Identity (IMEI) number that allows the service provider to identify the specific device used by a customer. Based on my review of Verizon records, [redacted] has been the subscriber of telephone number [redacted] since approximately 2012, and has continuously used the **Subject Phone** (assigned IMEI number 357202093093541) since at least approximately December 2018.

29. According to Apple and Verizon records, the **Subject Phone** has 512 gigabytes of storage capacity, which is the largest storage capacity that Apple offers for the iPhone XS model.

30. Based on my training and experience, I know that the only way that text messages (both SMS and MMS) sent or received over Apple iPhones can be removed

from the device is through manual deletion. Based on my training and experience, most iPhone users do not manually delete text messages (at least as a routine matter) because it is relatively labor intensive and, in most cases, unnecessary from a storage capacity standpoint. Because the **Subject Phone** has 512 gigabytes of storage capacity—which is an enormous amount of storage space for a personal phone—I believe it is highly unlikely that [redacted] has exceeded the **Subject Phone**'s storage capacity limitations such that he would have been forced to manually delete text messages to create extra storage space on his phone.

II. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

31. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence,

he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

32. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

33. In addition, electronic storage media such as a computer, its storage

devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

34. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor,

which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and

experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Face ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using Face ID for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person

may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

III. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

35. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure,

this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

36. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as

set forth in Attachment B;

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

37. The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

IV. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH [redacted]

38. Based on my training and experience, I know that it is customary for individuals who use cellular telephones to carry the devices on their person.

39. In particular, based on the facts described above, there is probable cause to believe that [redacted] is carrying the **Subject Phone** on his person. Specifically, the facts show that [redacted] uses the **Subject Phone** multiple times per day, including when [redacted] is away from his home or office. Further, subscriber records confirm that, as of August 4, 2021, [redacted] was still using the **Subject Phone**.

40. Therefore, the warrant in support of which this affidavit is submitted also seeks authorization to search the person of [redacted] for the **Subject Phone**.

V. CONCLUSION

41. Based on the above information, I respectfully submit that there is probable cause to believe that federal program bribery offenses, in violation of Title 18, United States Code, Section 666(a)(1)(B) and 666(a)(2), have been committed, that evidence relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Phone**, as further described in Attachment A, and that the **Subject Phone** is carried on the person of [redacted] I therefore respectfully request that this Court issue a search warrant for (1) [redacted] person (as more particularly described in Attachment A1) for purposes of locating and seizing the **Subject Phone** (as more particularly described in Attachments B1 and A2); and (2) the **Subject Phone**, authorizing the seizure of the items described in Attachment B2, pursuant to the protocol described in the addendum to Attachment B2.

FURTHER AFFIANT SAYETH NOT.

Gregory B. Linder by

Gregory B. Linder
Special Agent
Federal Bureau of Investigation

Sworn to and affirmed by telephone 13th day of August, 2021

Honorable GABRIEL A. FUENTES
United States Magistrate Judge

ATTACHMENT A2

DESCRIPTION OF ITEM TO BE SEARCHED

1. The gray Apple iPhone XS bearing IMEI number 357202093093541 and assigned telephone number [redacted].

ATTACHMENT B2

LIST OF ITEMS TO BE SEIZED

Evidence concerning violation of Title 18, United States Code, Section 666(a)(1)(B) and 666(a)(2), as follows:

1. Any and all MMS messages sent to or from the **Subject Phone** between February 2019 and July 24, 2020 that relate to the following:

a. Items related to the Project.

b. Items related to official acts taken or caused by [redacted] related to the Project and/or on [redacted] benefit or behalf.

c. Items related to Development Company 1, Development Company 2, Developer 1, Developer 2, or [redacted]

d. Items related to meetings between [redacted] and [redacted]

e. Items related to renovations, improvements, and/or other construction work at [redacted] [redacted] office.

f. Items related to benefits or things of value given by, or on behalf of, [redacted] to [redacted] and benefits or things of value given by, or on behalf of, [redacted] to [redacted]

g. Items related to the identity of the user or users of the **Subject Phone**.

2. During the execution of the search of [redacted] and the **Subject Phone**, as described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [redacted] to the fingerprint scanner of the

Subject Phone; (2) hold the **Subject Phone** in front of [redacted] face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

ADDENDUM TO ATTACHMENT B2

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.